S a D S a a (D a)

P

The purpose of this security standard is to ensure a consistent understanding of the concept of Segregation of Duties (SoD) and compliance with requirements and

applicable regulations. These requirements serve to assist in protecting the confidentiality, integrity, and availability of information.

S

Segregation of Duties serves to reinforce control measures through clear roles and responsibilities, ensuring that no single person has complete control over a transaction from start to finish. This promotes accountability and helps prevent mistakes, fraud, and other irregularities. By separating duties, each employee gains a better understanding of their responsibilities and can focus on their tasks without worrying about overlapping responsibilities or conflicts of interest. This, in turn, promotes transparency and assists in maintaining the integrity of operations within the organization.

The organization is required to adhere to the regulatory mandate of implementing Segregation of Duties across all processes, procedures, and supporting infrastructure. For other processes and procedures, the implementation of these requirements should be based on a risk assessment.

This security standard outlines the framework and high-level requirements of SoD but does not prescribe how it should be implemented or the detailed linkage between organization, role types, sub-roles, access rights, and job descriptions.

G a S a a

SODSTD 1.1

To prevent any individual from bypassing intended controls or controlling an entire process independently, key roles, duties, and areas of responsibility must be adequately segregated.

SODSTD 1.2

The framework is based on the concept of roles (which equates to duties) and the allocation of all users (employees, consultants, etc.) to one of the three primary role types:

- IT Development
- IT Operations

- Business

The allocation to one of these three areas must be reflected in their assignment of access rights and organizational allocation. Ensure that IT development, IT operations, and business usage are separated, and no individual has access rights that relate to more than one of these three areas. Incompatible duties within primary roles will be addressed with sub-roles.

SODSTD 1.3

The principle of SoD should be applied to mitigate the risk of mixing different functions. No individual should have the ability to initiate and authorize an event or handle all the steps in a process chain. This requirement must be reflected in the allocation of access rights. SoD must be implemented when assigning roles for access control, including access request, access authorization, and access administration.

SODSTD 1.4

An administrator is not allowed to grant any authorization to themselves. Effective controls, monitoring, or review procedures must be established for this purpose.

SODSTD 1.5

Each department/unit is responsible for creating relevant sub-roles, so long as these sub-roles follow the principles of the primary roles.

SODSTD 1.6

Where adequate segregation cannot be established, compensating controls must be implemented and should include, at a minimum, an approval/exemption process and close supervision/continuous auditing.

R T

IT D

Applies to activities including developing and changing source code, configuration files, database schemas, and operating in the Development and Test environments.

IT O a

Applies to activities including deploying changes to configuration/applications/data, running and monitoring services/jobs, supporting infrastructure or applications, and administrating IT services in production.

B

Applies to activities conducted by service users who use approved business applications for their role to initiate a transaction, provide approval or authorization, report or record, etc., to fulfill a part of a business process.

S b-R

SODSTD 1.11

Further division is required based on any identified incompatible duties within each of the primary roles.

SODSTD 1.13

Establishment of a control environment that supports SoD requires a combination of sub-roles that permit an individual to participate in different processes, provided any incompatible combinations are eliminated.

SODSTD 1.14

It is required that access control mapping is created that includes primary roles.

SODSTD 1.15

Combinations of sub-roles lead to job roles. SoD conflicts should be assessed at the job role level as well as at the access control level.

S b-R E a

B A a

- Sub-role to the primary role: Business.

- Designed to ensure that analysts throughout the organization can have read access to the data they need if they adhere to the "need to know" principle.
- Can be organized in any organizational unit (including development and operational units) without constituting a violation of the organizational SoD.
- Cannot assume any other main or sub-role.

P b Ta /A R :

- Actual coding (access to source code repositories, etc.).
- Privileged access or operational tasks in any environments in scope of SoD.
- Generate business transactions (write access to any production environment in scope of SoD).

F S a D

- Sub-role to the primary role: IT Developer.
- Designed to ensure that full stack developers have access to relevant tools and systems that support their work.
- Tend to have privileged access rights, allowing them to have write access to source code.
- Cannot assume other main or sub-roles without violating organizational SoD.

A a R

SODSTD 1.7

Based on requirements, there must be a SoD between the primary roles of Business, IT Development, and IT Operations.

SODSTD 1.8

Individuals cannot have duties spanning beyond one of the primary role types. In cases where duties are incompatible, they must be handed over to another individual.

SODSTD 1.9

All managers must assign their team members to the role that represents their primary duties. Any additional incompatible duties must be resolved.

SODSTD 1.10

Assigned IT access rights must be compared with the relevant role to identify any incompatible duties. In such cases, these duties must be handed over to another unit, and related access rights must be removed.

SODSTD 1.11

Access rights must be adjusted to align with the SoD roles. Additionally, any IT access rights that exceed an individual's duties and "need to know" basis must be eliminated.

I a a C a

1. **T a a A a** : Conduct regular training sessions and awareness campaigns to educate employees and managers about SoD policies and best practices.
2. **M a A** : Implement continuous monitoring mechanisms and maintain comprehensive audit trails for all access and role changes.
3. **I Ma a** : Develop a detailed incident response plan for handling SoD violations, including steps for investigation, remediation, and reporting.
4. **M a R** : Define KPIs and implement regular reporting mechanisms to track compliance with SoD requirements and identify areas for improvement.
5. **S a I** : Involve cross-functional teams in the development and implementation of SoD policies and establish a feedback mechanism to gather input from stakeholders.

By adhering to these standards and continuously improving the SoD framework, the organization can ensure the integrity, confidentiality, and availability of its information and processes.